Seguridad informática

Biblioteca/CRAI de la Universidad Pablo de Olavide
Formación en Competencia Digital

UNIVERSIDAD PABLO DE OLAVIDE SEVILLA

Universidad Pablo de Olavide.
Biblioteca/CRAI. Formación de Usuarios.

Visita la guía online

Fecha de creación:20/11/2020
Versión:1.0

Tabla de contenido

Recuerda la metodología del curso

* Recuerda leer y repasar la **metodología** del curso y seguir los pasos que se explican en la **guía**.

* El **Foro** "Competencia Digital: dudas y consultas" está para resolver tus dudas ¡Utilízalo!

* La **Encuesta de satisfacción** nos ayuda a mejorar, rellénala y tendrás disponible la **Evaluación final**

* Para la **Evaluación final** consulta la información disponible en la **guía del curso.**

¿Qué voy a aprender?

Pasamos muchas horas delante de diferentes dispositivos digitales (pc, tablet, móvil...); según Apple desbloqueamos nuestro móvil una media de 80 veces al día, lo que hace que pasemos más de 4,7 horas consumiendo información visual o digital.

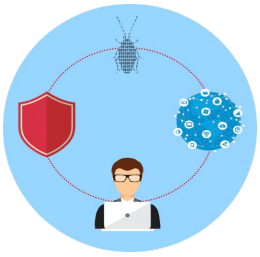
Pero, cuidado, el mundo digital es un campo de batalla abierto donde, si no te proteges bien, acabarás derrotado ante la invasión a tu persona.

- ¿Tienes control de las aplicaciones que usas?
- ¿Tienes contraseñas seguras?
- ¿Eres cuidadoso con tus redes sociales y tienes bien configurados tus niveles de privacidad?
- ¿Eres consciente de que cuantos más amigos tengas en Facebook más expuesto estás a terceros?
- ¿Sabes qué es el *phishing*?
- ¿Eres de los que anotan su contraseña en papeles o libretas en su escritorio?...

Si a las preguntas anteriores has contestado "NO" y normalmente haces lo que dice esta simpática chirigota callejera, tienes un problema: tu seguridad está comprometida y eso te hace ser muy vulnerable.

Con esta guía te vamos a dar algunas pautas sobre cómo estar seguros digitalmente y tener una buena armadura protectora. Porque por mucha armadura que haya (sistemas de seguridad tales como: antivirus, contraseñas, acceso por huella, sistemas de prevención de malware, antispyware...), eres tú quien puedes garantizar tu propia seguridad y si decides o no estar protegido.

¿Qué es la Seguridad Digital o Ciberseguridad?



La **seguridad informática**, también conocida como ciberseguridad o seguridad de tecnologías de la información, es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger infraestructura computacional (activos de la organización) y todo lo relacionado con esta, así como a los propios usuarios de la misma.

¿Desconocimiento, ignorancia, exceso de confianza?

La falta de una cultura de seguridad digital es un asunto que preocupa a empresas, universidades, organizaciones e instituciones.

Por ejemplo...

Nadie quiere recordar 10 contraseñas diferentes, con letras, números y caracteres especiales ¿cuántos pueden incluso? Lo bueno es que no hay que hacerlo necesariamente. Hay administradores de contraseñas que guardan una copia segura de estas en un ordenador o en la nube. Usar estas herramientas es una capa extra de defensa. Y si vas a hacer un respaldo de esta información en un papel, no es sabio dejarlo a la vista de todo el mundo en una nota pegada en la pantalla del ordenador. Hay que hacerlo; pero hacerlo bien.

Recuerda que...

Nosotros, los usuarios, somos la pieza clave del puzle de la ciberseguridad. Es la persona quien gestiona la información; la modifica, la trasmite, la elimina y la procesa.

Aquí te dejamos el siguiente vídeo de concienciación; si sustituyes "empleado" por "usuario", te servirá de ayuda para ser una persona más consciente de que la ciberseguridad, al fin y al cabo, depende de las personas, de los usuarios finales.

Kit de concienciación en ciberseguridad

Tal y como insiste el Instituto Nacional de Ciberseguridad (INCIBE) si queremos estar protegidos con cierta confianza, ***"debemos conocer y concienciarnos de los puntos más importantes o clave de seguridad e implantar las medidas oportunas de seguridad para la adecuada protección de la información a la hora de desempeñar la actividad profesional"*** (INCIBE, 2017).

¡Ojo!...

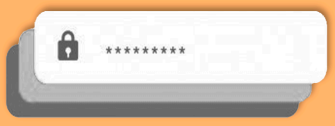
Evita el uso de equipos no corporativos para acceder a servicios de la Olavide. Si accedes al correo corporativo desde tu equipo personal, no descargues ficheros al equipo.

¡Toma nota...!

Debes proteger tu mesa de estudio manteniéndola "limpia" de papeles con contraseñas o datos que contengan información sensible.

No uses tu usuario y contraseña institucional de la Universidad en aplicaciones de uso personal o viceversa.

Usa siempre una clave de acceso, patrón, y bloqueo automático en tu móvil (y si tienes posibilidad) acceso mediante huella dactilar o reconocimiento facial.

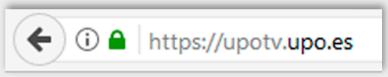


Las contraseñas deben ser secretas y únicas, no las anotes, compartas o reutilices.

Navega de forma segura y evita acceder a páginas web de las que desconfíes y no fiables.

Utiliza el correo electrónico de forma segura y elimina o informa al CIC (centro de informática y comunicaciones de la UPO) de todo correo sospechoso que recibas. Evita correos en cadena.

No hagas clic en enlaces o links raros o sospechosos. Es mejor reproducir la dirección en la barra del navegador.

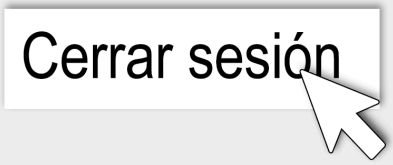


Protege la información y realiza copias de seguridad de información sensible.

Si viajas, no mandes información sensible a través de wifis no confiables.

No introduzcas discos extraibles de terceros sin antes hacer un escaneo con un antivirus. Ademas evita transportar información sensible en estos dispositivos.

Cada vez que termines de usar el Aula Virtual tu correo electrónico, bases de datos, etc. con tus creedenciales, no olvides cerrar sesión. También recuerda bloquear tu equipo cuando te ausentes.



Protección de información y datos personales

¿Cómo gestionas tus datos personales?

Debemos tener sumo cuidado a la hora de tratar con nuestros datos y los de terceros. En nuestras empresas todos manejamos datos personales de clientes, proveedores y empleados. Saberlos gestionar y proteger nos dará ventaja sobre nuestros competidores.

Reglamento General de Protección de Datos

Recientemente ha entrado en vigor el **Reglamento General de Protección de Datos** que viene a armonizar la protección de los ciudadanos a este respecto en toda Europa.

¿Sabes qué es el LOPD?

Es la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos de Carácter Personal y garantía de los derechos digitales. Si quieres conocer de qué trata esta ley y de qué nos protege haz clic en:

Más info

Riesgos y amenazas en entornos digitales

Cada vez hay más **crisis reputacionales**: momentos en los que la percepción de otros sobre una persona u organización se ve comprometida o puesta en entredicho por el conocimiento de una información concreta. Pero la solución no pasa por evitar estar en la red -pueden hablar de tu empresa y de ti sin que estés en ella-. La actitud aconsejada es actuar de forma apropiada, mantenerse alerta y tener un protocolo de actuación ante posibles amenazas. Nuestra reputación online está en juego por lo que es importante conocer los posibles riesgos desde el punto de vista de la seguridad. ¿Sabemos reconocer una **suplantación de identidad**? ¿Qué hacer cuando publican **información falsa sobre la empresa**? (MACARIO, 2016)

En esta infografía puedes tener más conocimiento resumido:

Toma nota...

El robo de datos y de información empresarial es ahora más fácil que nunca; por ejemplo, a través del WIFI de la empresa. Los "piratas" aprovechan que muchas empresas trabajan con sus documentos en la nube o con soluciones de gestión documental en línea, esto hace más vulnerable la documentación de la empresa. El problema viene dado por las fugas de información estratégica con las que las empresas pierden información de vital importancia para garantizar la viabilidad de sus negocios y, en algunos casos, pueden ocasionar la vulneración de la privacidad de las personas, cuyos datos estén contenidos en los documentos sustraídos.

¿Qué es el phishing y cómo prevenirlo?

"He recibido un correo electrónico solicitándome que actualice los datos personales de mi cuenta corriente haciendo clic en un enlace, pero me extraña que la URL de mi banco no sea la misma de siempre. He llamado al banco y me han dicho que es una estafa conocida como phishing." (INCIBE, 2017).

Entre los riegos con los que nos podemos encontrar cuando hacemos uso de Internet está el phishing, una técnica usada por ciberdelincuentes para obtener información personal y bancaria de los usuarios suplantando a una entidad legítima como puede ser un banco, una red social, una entidad pública, etc.

¿Cómo funciona el phishing?

Los ciberdelincuentes captan nuestra atención con alguna excusa con el fin de redirigirnos a páginas web fraudulentas que simulan ser legales y originales del servicio que ofertan. Cualquier sistema que permita el envío de mensajes puede ser usado como medio para intentar robar nuestra información personal. En algunos casos pueden llegar intentos de robo de nuestra información personal a través de emails, mensajes SMS o MMS (*smishing*), de la misma manera que por cualquier herramienta de mensajería instantánea (*WhatsApp*, *LINE*, etc.) o red social.

(INCIBE, 2017)

¿Qué hacer si lo detectas?

- No contestes en ningún caso a estos correos. Si tienes dudas pregunta directamente en el Centro de Informática y Comunicaciones (CIC) a través de la cuenta: seguridadti@upo.es.
- No accedas a los enlaces facilitados en el mensaje ni descargues ningún documento adjunto.
- Elimínalo y, si lo deseas, alerta a tus contactos sobre este fraude.

¿Cómo prevenirlo?

- Sé precavido ante los correos que aparentan ser entidades bancarias o servicios conocidos con mensajes del tipo:
  - Problemas de carácter técnico de la entidad.
  - Problemas de seguridad en la cuenta del usuario.
  - Recomendaciones de seguridad para evitar fraudes.
  - Cambios en la política de seguridad de la entidad.
  - Promoción de nuevos productos.
  - Vales descuento, premios o regalos.
  - Inminente cese o desactivación del servicio.
- Sospecha si hay errores gramaticales en el texto.
- Si recibes comunicaciones genéricas dirigidas a "Estimado cliente", "Notificación a usuario" o "Querido amigo", es un indicio que te debe poner en alerta.
- Si el mensaje te obliga a tomar una decisión en unas pocas horas, es mala señal. Contrasta directamente si la urgencia es real o no con el servicio a través de otros canales.
- Revisa que el texto del enlace coincide con la dirección a la que apunta.
- Un servicio con cierto prestigio utilizará sus propios dominios para las direcciones de email corporativas. Si recibes la comunicación desde un buzón de correo tipo @gmail.com o @hotmail.com, no es buena señal.

No hagas clic en enlaces que recibas a través de un mensaje para acceder a un sitio web en el que te tienes que identificar o facilitar información personal (INCIBE, 2017).

Contraseñas

"¡Qué locura! Cada vez que me registro en un nuevo servicio tengo que facilitar una contraseña, y como uso tantos (Facebook, Instagram, PayPal, Gmail...), no soy capaz de gestionar mis contraseñas de acceso adecuadamente, acabo siempre usando la misma para facilitarme la vida, aunque he oído que **eso no es una buena práctica**. ¿Qué puedo hacer?"

No es una buena práctica utilizar la misma contraseña para acceder a distintos servicios, si en algún momento tu contraseña se viera comprometida, el riesgo para tu información personal sería mucho mayor, ya que entregas las contraseñas corporativas en servicios con menos garantías.

Aunque la tarea de generar y mantener contraseñas seguras en ocasiones es un proceso pesado y molesto, es una tarea necesaria si queremos impedir que otras personas puedan acceder a nuestra información, invadiendo nuestra privacidad y derivando en problemas de suplantación de identidad, ciberacoso, problemas económicos, etc.

Los hackers disponen de algunas herramientas para descifrar contraseñas. Pero no debemos alarmarnos. Siguiendo los consejos que veremos en el siguiente vídeo de INCIBE, podremos crear contraseñas robustas y seguras que queden lejos de su alcance.

Infografía sobre consejos y recomendación para elegir tus contraseñas

Consejos y recomendaciones

Qué nadie adivine tus contraseñas

- Elige **contraseñas fuertes** o robustas de al menos 8 caracteres y compuesta por:
  - mayúsculas (A, B, C…)
  - minúsculas (a, b, c…)
  - números (1, 2, 3…)
  - y caracteres especiales ($, &, #...)
- **NO** utilices contraseñas fáciles de adivinar como: "12345678", "qwerty", "aaaaa", nombres de familiares, matrículas de vehículos, etc.
- **NO** compartas tus contraseñas. Si lo haces, dejará de ser secreta y estarás dando acceso a otras personas a tu privacidad.
- **NO** uses la misma contraseña en varios servicios.

Utiliza patrones para crear y recordar tus claves

- Elige un símbolo especial: "&".
- Piensa una frase que no se te olvide nunca y quédate con sus iniciales: "En un lugar de la Mancha" -> "EuldlM".
- A continuación, selecciona un número: "2".
- Concatena todo lo anterior y tendrás una buena contraseña:

EJEMPLO: **&EuldlM2**

- Símbolo especial: &
- Regla nemotécnica: "En un lugar de la Mancha"
- EuldlM
- Número: 2

TRUCO:
Si al patrón anterior, le añades un elemento diferenciador (por ejemplo, la inicial del sitio web, producto, aplicación, juego o servicio), ¡Tendrás una contraseña diferente para cada uno!

Si eres olvidadizo, usa un gestor de contraseñas

Cuando manejas muchas contraseñas y no eres capaz de recordarlas todas, utiliza un **gestor de contraseñas**. Es un programa que te permite almacenar de forma segura tus claves de acceso a los diferentes servicios.

- Solo necesitas recordar la clave de acceso al gestor de contraseñas, conocida como clave maestra, para consultar el resto de tus contraseñas.
- Eso sí, si la olvidas no podrás consultar el resto, por tanto, memorízala bien en tu cabeza.

Cuatro estaciones, cuatro contraseñas

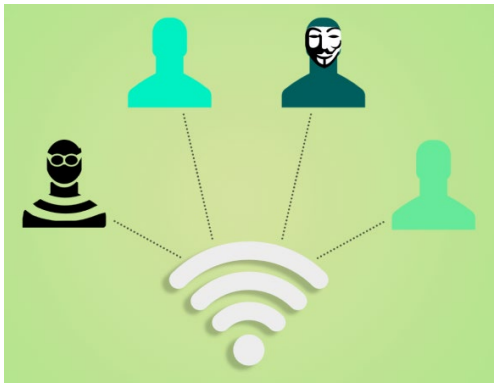
A pesar de lo fuerte o robusta que sea tu contraseña, con el paso del tiempo puede verse comprometida.

- **Cambia tus contraseñas periódicamente.**

El maravilloso y peligroso mundo de la wifi

Cada vez son más los dispositivos de uso doméstico que disponen de conexión inalámbrica o wifi: frigoríficos, televisores, impresoras, etc. También el número de dispositivos móviles y ordenadores que utilizamos en nuestro domicilio, por tanto, necesitamos proteger nuestra vivienda para que ningún vecino o "ladrón cibernético" se cuele en ella a través de la conexión y:

- Nos quite nuestro más preciado tesoro: "el ancho de banda" y "nuestra información personal".
- Se cuele en nuestros equipos conectados (la *Smart TV*, tabletas, móviles, etc.)
- Nos ocasione un verdadero problema legal con nuestra distribuidora de Internet ante acciones ilícitas de terceros ya que la IP es tuya y el contrato está a tu nombre.



Otra cosa a tener en cuenta es que las redes wifi p**úblicas** (aeropuertos, cafeterías, bibliotecas, etc.) pueden no ser seguras ya sea porque no cifran la información que se transmite a través de ellas, o porque desconocemos quién está conectado a esa misma red y con qué fines.

Toma nota...
Siempre que vayas a realizar trámites online evita hacerlo desde redes wifi públicas. Conéctate mejor con el 3G/4G del móvil o desde la wifi de tu casa, pero sin olvidar comprobar primero si tu red wifi está correctamente configurada para evitar que desconocidos se conecten a ella.

Hablando de redes wifi en sitios públicos, por ejemplo, tu Universidad o su biblioteca, debes saber que hay una red segura conocida como "Eduroam"; es a ésta a la que tendrás que conectarte, aunque tendrás que pedir permiso para su instalación y acudir al CIC (Centro de informática y Comunicaciones) para que te ayuden a registrarte en ella. En el enlace anterior tienes toda la información.

Eduroam

¿Sabes qué significa?

Eduroam (Education roaming) es la iniciativa que crea un espacio único de movilidad entre la comunidad académica y de investigación a lo largo de todo el mundo.

Este servicio, permite al usuario tener conectividad en cualquier centro "eduroam" (como la Universidad Pablo de Olavide) sin necesidad de reconfigurar continuamente sus dispositivos.

Es una iniciativa coordinada a nivel nacional por **RedIRIS,** que en base a unas políticas comunes de uso ofrece un servicio de movilidad a los usuarios de dichas instituciones.

Sigue estos consejos que marca INCIBE:

Configura correctamente la conexión wifi:

1. *Averigua la dirección IP de tu router.*
2. *Accede a su página de administración.*
3. *Cambia la contraseña que trae por defecto de acceso a la administración.*
4. *Modifica el nombre de la wifi o SSID.*
5. *Configura la wifi para que use cifrado WP2.*
6. *Crea una contraseña robusta de acceso a la wifi.*
7. *Consulta la dirección MAC de tus dispositivos y aplica el filtrado por MAC en el router.*
8. *Apaga el router cuando no lo estés utilizando.*

Aunque te parezca que estas cosas solo les pasan a los demás y que tu red wifi nunca va a ser objetivo de un atacante, debes ser prudente y aplicar todas las medidas de seguridad que están a tu alcance para que un intruso no utilice tu conexión y no te cause ningún problema.

Y además, protege tus dispositivos:

- *Asegúrate que están actualizados a su última versión.*
- *Instala una herramienta antivirus.*
- *No navegues ni uses el PC con usuario administrador para las tareas rutinarias.*
- *Usa buenas contraseñas.*
- *No ejecutes programas o sigas enlaces que te lleguen por correo y cuyo contenido te parezca extraño o sea de origen dudoso para evitar fraudes y malware.*
- *No conectes dispositivos extraíbles cuya procedencia y contenido ignoras.*
- *Si el dispositivo dispone de cámara, tápala cuando no la estés usando.*

La configuración por defecto del router no es siempre la más apropiada

Para saber más sobre la seguridad con las redes wifi visualiza este vídeo

Virus: Cómo prevenirlos y evitarlos

Malware es la forma genérica de llamar a cualquier programa que se ejecuta sin autorización y con objetivos maliciosos (virus, troyanos, gusanos…). Para ser estrictos, virus se reserva a cierto tipo de malware con capacidad de propagación e infección. En muchos contextos se usa la palabra virus como genérica cuando no es un uso correcto, aunque sí aceptado y difundido.

¿Sabes cuántos tipos de virus puedes encontrarte?

Entra en cada una de la fichas, para conocer a través de la infografía tan divertida e ilustrativa que ha elaborado la **Oficina de Seguridad del Internauta**, cómo actúan cada uno de ellos y así poder localizarlos.

VIRUS

TROYANO

BichosNet Busca Inicio Perfil Amigos Cuenta

Muro
Información
Fotos
Preguntas
Amigos

Páginas
Hipica
Troya
Caballos

TROYANO

Información del perfil

Información Básica
Soy un malware eficaz y muy usado. Mi gran arma es que no soy lo que parezco ser

Aficiones
- Me gusta la leyenda del caballo de Troya
- Darle el control de tu ordenador a mi amo
- Cada vez me gustan más los móviles. Puedo acceder a toda su información.
- Juntarme con otros troyanos y hacer fiestas en las botnets

Lugares de Residencia
Aplicaciones y archivos del sistema operativo.

Orígenes
Provengo de adjuntos de correos y programas que parecen inofensivos

Tiene una relación
Con puertas traseras (backdoors) y otros troyanos en botnets

No Me Gusta
- Los antivirus y anti-troyanos
- Que no se fíen de adjuntos sospechosos
- El software legítimo. Yo prefiero programas piratas

GSANO

BichosNet Busca Inicio Perfil Amigos Cuenta

Muro
Información
Fotos
Preguntas
Amigos

Páginas
Mariposas

GUSANO

Información del perfil

Información Básica
Mi misión principal es multiplicarme y propagarme por las redes. Solo necesito tu ayuda para arrancar. ¡Luego nadie puede pararme!

Aficiones
- Molestar saturando y colapsando las redes inútilmente
- Replicarme y extenderme por otros ordenadores

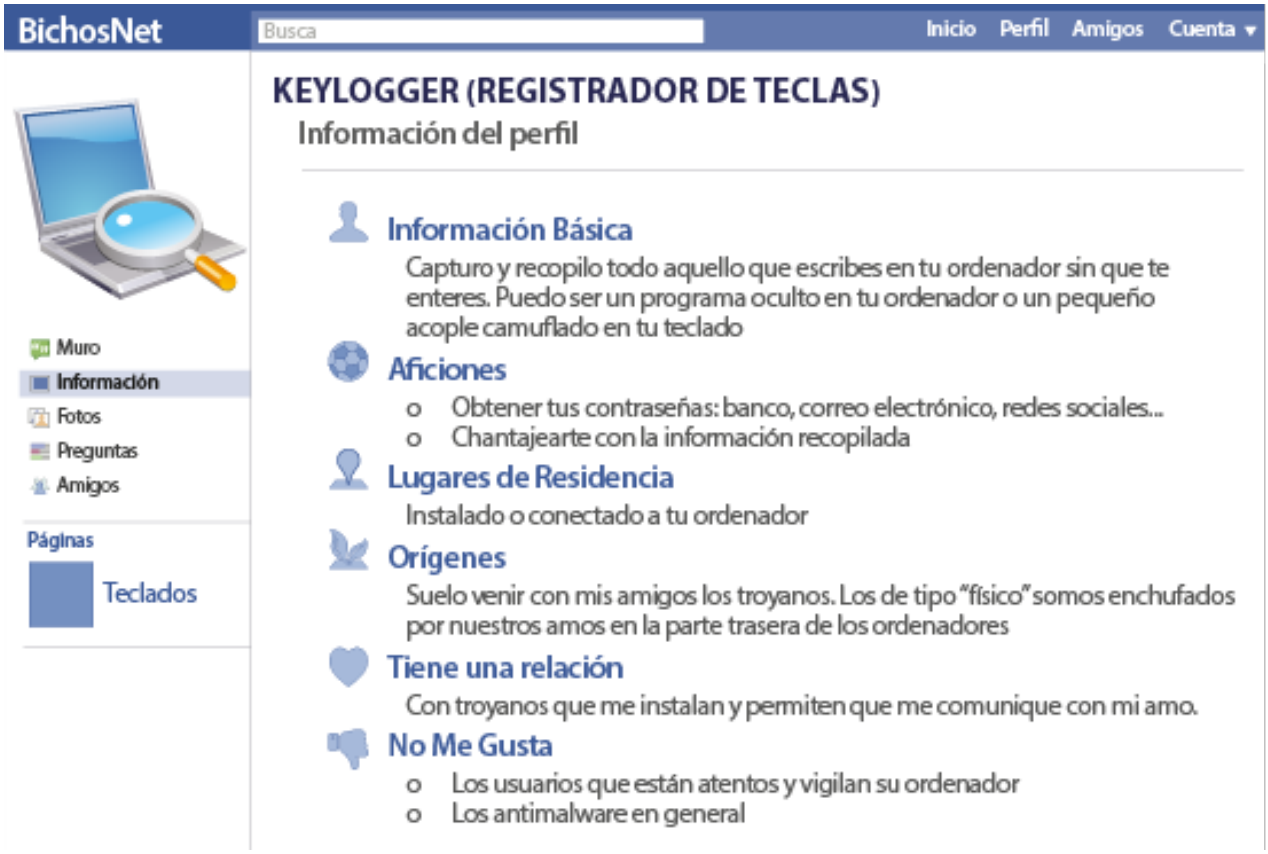
Lugares de Residencia
En la memoria RAM de tu ordenador. No necesito infectar otros ficheros

Orígenes
Provengo de otros ordenadores de tu red o directamente desde Internet. Mi pariente más famoso es El Gusano de Morris

Tiene una relación
Con internet y las redes de ordenadores

No Me Gusta
- Los cortafuegos (firewalls) que no me dejan expandirme por las redes
- Los antimalware en general
- Los chats seguros

Keylogger (Registradores de teclas)



Ransomware (Secuestradores)

Rogueware (Falsos antivirus)

Spyware (Program Espía)

¿Cómo puedo evitarlos?

1. En la UPO, vigila e informa al CIC de comportamientos no deseados de tu equipo: lentitud excesiva, pérdida de red, aparición de anuncios o mensajes no solicitados.
2. En tus equipos de uso personal instala un **antivirus** y un **cortafuegos** y mantenlos actualizados. No instales programas que desconozcas. Para descargas, acude siempre a las páginas de los proveedores originales.
3. Mantén tu equipo constantemente actualizado.
4. Nunca ejecutes un programa o sigas un enlace que te llegue por correo y parezca extraño.
5. No ejecutes ficheros de dudoso origen.
6. No conectes a tu equipo un USB cuya procedencia ignoras.
7. Utiliza el sentido común; sé precavido ante cualquier cosa que te parezca sospechosa (OSI, 2017).

Copias de seguridad

Podemos considerar como una amenaza más la pérdida de información personal de nuestros dispositivos por el borrado accidental o intencionado por terceros. Por tanto, debemos ser muy cuidadosos y preventivos con nuestra información sensible que bajo ningún concepto queremos perder: fotos, archivos, música, documentos, facturas, vídeos, etc.

Pero no te preocupes, todo tiene solución y la mejor de todas, como siempre, es la **prevención**. La **OSI**, nos ofrece estas recomendaciones que te sugerimos las tomes como un hábito o patrón en tu día a día, si no lo hacías antes.

Consejos y Recomendaciones

(OSI, 2017)

Herramientas gratuitas para tu protección y seguridad

La Oficina de Seguridad del Internauta (**OSI**) pone a nuestra disposición una serie de herramientas gratuitas que nos ayudarán a proteger nuestros dispositivos.

Ten en cuenta que…

Esta información que ves en este punto es para los equipos personales, para los equipos corporativos no deben instalarse aplicaciones similares a las plataformas corporativas: antivirus, cortafuegos, etc.

Las herramientas están clasificadas en cuatro grandes bloques:

- **Antirrobo, seguridad y protección de acceso** (acceso remoto, cortafuegos y antirrobo).
- **Privacidad y seguridad de datos** (cifrado y gestión de contraseñas, control parental, privacidad y navegación).
- **Mantenimiento** (copias de seguridad, gestor de tareas, mantenimiento y limpieza).
- **Protección, análisis y desinfección** (antivirus, análisis online y cleaners, análisis de tráfico).

En función de nuestra necesidad, debemos buscar en uno u otro bloque. Haz clic en la imagen y podrás ver todas las herramientas disponibles y totalmente gratuitas.

Toma nota...
Si no encuentras lo que buscas y necesitas ayuda, no dudes en escribir a la OSI través del formulario de contacto, los técnicos te ayudarán.

Además, recuerda que...

La UPO también puede ayudarte a través del Centro de Informática y Comunicaciones CIC y más concretamente su oficina de Seguridad Digital

La UPO vela por tu seguridad

Como estudiante, docente, investigador/a o visitante, debes saber que hay todo un equipo de profesionales que te ayudarán y velarán por tu seguridad digital en tu entorno académico. Aquí tienes su contacto:

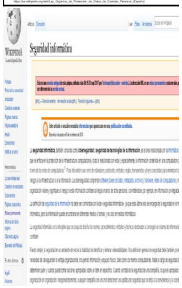
Más info

Si quieres estar informado de forma permanente te animamos a que participes en las campañas de concienciación que llevan a cabo desde el Centro de Informática, síguelos en las redes sociales y permanece atento a sus mensajes. Acércate al CIC y solicítales información.

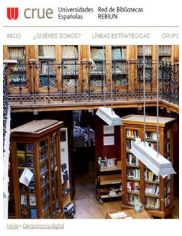
Bibliografía

Certificados digitales: una herramienta muy útil a tu alcance por CI2CRUE
Fecha: 5 noviembre 2013.
En: YouTube [vídeo en línea]. Disponible en: https://youtu.be/8ab88NLomY8 [Consulta: 8 junio 2020].

Ley Orgánica de Protección de Datos de Carácter Personal por colaboradores de Wikipedia
Fecha: 2017.
En: Wikipedia, la enciclopedia libre. Disponible en: https://es.wikipedia.org/wiki/Ley_Org%C3%A1nica_de_Protecci%C3%B3n_de_Datos_de_Car%C3%A1cter_Personal_(Espa%C3%B1a) [Consulta: 8 junio 2020].



Seguridad informática por colaboradores de Wikipedia
Fecha: 2017.
En: Wikipedia, la enciclopedia libre. Disponible en: https://es.wikipedia.org/w/index.php?title=Seguridad_inform%C3%A1tica&oldid=102021318. [Consulta: 8 junio 2020].



Objetos de aprendizaje por CRUE y Rebiun
En: CrueCRUE, Universidades Españolas. Red de bibliotecas de Rebiun [en línea]. Disponible en: http://www.rebiun.org/competenciadigital/Paginas/objetosdeaprendizaje.aspx [Consulta: 9 junio 2020].

Chirigota contraseña por Gómez, Ana
Fecha: 9 marzo 2017.
En: YouTube [vídeo en línea]. Disponible en: https://youtu.be/hMG4YI7d3qU [Consulta: 8 junio 2020].

Desarrollar cultura en seguridad por INCIBE (Instituto Nacional de Ciberseguridad)
Fecha: 2017.
Disponible en: https://www.incibe.es/protege-tu-empresa/que-te-interesa/desarrollar-cultura-en-seguridad [Consulta: 9 junio 2020].

Jornadas INCIBE "Espacios de Ciberseguridad" para estudiantes de secundaria por INCIBE (Instituto Nacional de Ciberseguridad)
Fecha: 2017.
Disponible en: https://www.incibe.es/jornadas-incibe-espacios-ciberseguridad/estudiantes [Consulta: 9 junio 2020].

Kit concienciación para empresas por INCIBE (Instituto Nacional de Ciberseguridad)
Fecha: 20 enero 2015.
En: YouTube [vídeo en línea]. Disponible en: https://youtu.be/-3AhTYiDTIE [Consulta: 9 junio 2020].

Privacidad y seguridad en Internet por INCIBE (Instituto Nacional de Ciberseguridad)
Fecha: 2017.
Disponible en: https://www.osi.es/sites/default/files/docs/guiaprivacidadseguridadinternet.pdf [Consulta: 9 junio 2020].

Configurar Eduroam en Windows 7, 8, 8.1 y 10 por Informático Vitoria
Fecha: 2016.
En: YouTube [vídeo en línea]. Disponible en: https://youtu.be/1GGfd7z2HYk [Consulta: 9 junio 2020].

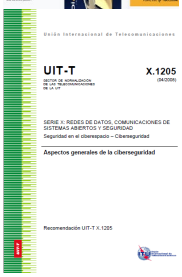
6 amenazas para la identidad digital de tu empresa #infografia por Macario, Andrés
Fecha: 2016.
Disponible en: https://andresmacario.com/6-amenazas-para-la-identidad-digital-de-tu-empresa-infografia/ [Consulta: 9 junio 2020].

Certificados electrónicos personales, esos grandes desconocidos por OSI
Fecha: 2016.
En: OSI, Oficina de Seguridad del Internauta [en línea]. Disponible en: https://www.osi.es/es/actualidad/blog/2016/04/14/certificados-electronicos-personales-esos-grandes-desconocidos [Consulta: 9 junio 2020].

Fauna y flora del mundo de los virus por OSI
Fecha: 2014.
En: OSI, Oficina de Seguridad del Internauta [en línea]. Disponible en: https://www.osi.es/actualidad/blog/2014/07/18/fauna-y-flora-del-mundo-de-los-virus [Consulta: 9 junio 2020].

Herramientas por OSI
Fecha: 2017.
En: OSI, Oficina de Seguridad del Internauta [en línea]. Disponible en: https://www.osi.es/es/herramientas [Consulta: 9 junio 2020].

10 pasos para proteger los datos personales en la empresa por PIMETIC Informática
Fecha: 2014.
Disponible en: http://www.pimetic.com/es/2014/11/14/pasos-para-proteger-los-datos-personales/ [Consulta: 9 junio 2020].



Serie X: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad. Seguridad en el ciberespacio – Ciberseguridad. Aspectos generales de la ciberseguridad (04/2008) por Unidad Técnica de Telecomunicaciones
Fecha: 2008.
Disponible en: https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1205-200804-I!!PDF-S&type=items [Consulta: 8 junio 2020].

Actividades de práctica

Eduroam	Documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.
Centro de informática y comunicaciones UPO	Este servicio permite que estudiantes, investigadores y personal de las instituciones participantes tengan conectividad Internet a través de su propio campus y cuando visitan otras instituciones participantes
Troyano	Equipo de profesionales de la Universidad Pablo de Olavide que te ayudarán y velarán por tu seguridad digital en el entorno académico
Certificado electrónico	Soy un malware eficaz y muy usado. Mi gran arma es que no soy lo que parezco ser.
Seguridad informática	Es el conjunto de herramientas, políticas, conceptos, salvaguardas, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger la infraestructura computacional y todo lo relacionado con esta, así como a los propios usuarios de la misma
Phising	Los ciberdelincuentes captan nuestra atención con alguna excusa con el fin de redirigirnos a páginas web fraudulentas que simulan ser legales con el fin de robar nuestra información personal.

Repasando lo aprendido

El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger infraestructura computacional (activos de la organización) y todo lo relacionado con esta y a los propios usuarios de la misma, se conoce como:

- [ ] Identidad digital
- [ ] Ciberseguridad
- [ ] Phishing

¿Existen administradores de contraseñas que guardan una copia segura de estas en un ordenador o en la nube?

- [ ] Verdadero
- [ ] Falso

¿Cuáles son algunas de las principales amenazas de la identidad digital?

- [ ] La suplementación de identidad
- [ ] La publicación por terceros de informaciones falsas
- [ ] La utilización no consentidad de derechos de propiedad
- [ ] Todas son correctas

¿Qué es el LOPD?

- [ ] Ley Orgánica 3/2018 de 5 de diciembre Protección de Datos de Carácter Personales y garantía de los derechos digitales
- [ ] Reglamento General de Protección de Datos
- [ ] Ley Orgánica de Derechos personales

Según los consejos de ciberseguridad, cada vez que termines de navegar en una página con tus credenciales, debes cerrar la sesión

- [ ] Verdadero
- [ ] Falso

¿Qué es el phishing?

- [ ] El uso indebido de la imagen corporativa, marca u otros elementos por parte de terceros sin permiso del propietario
- [ ] La técnica usada para obtener información personal y bancaria de los usuarios suplantando a una entidad legítima como puede ser un banco, una red social o una entidad pública
- [ ] El uso de publicaciones por terceros de informaciones falsas que puede arruinar la reputación online de una persona o marca

Las redes wifi públicas (aeropuertos, cafeterías, bibliotecas, etc.) son seguras ya que cifran la información que se transmite a través de ellas y porque podemos ver quién está conectado a la red.

- [ ] Verdadero
- [ ] Falso

Un malware es la forma genérica de llamar a cualquier programa que se ejecuta sin autorización y con objetivos maliciosos (virus, troyanos, gusanos…).

- [ ] Verdadero
- [ ] Falso

¿Cuáles son las recomendaciones correctas para no perder nuestra información personal (fotos, vídeos, documentos, etc) de nuestros dispositivos?

- [ ] Has solamente una copia de seguridad en tu espacio de la nube
- [ ] Selecciona los archivos deseados, elige el soporte de almacenamiento donde los copiarás, haz la copia de seguridad y repite este proceso periódicamente.
- [ ] Selecciona los archivos que desees almacenar, crea una carpeta en el escritorio de tu ordenador y cópialos ahí.

Qué servicio responsable de la Universidad Pablo de Olavide vela por la seguridad informática de toda la comunidad universitaria

- [ ] Centro de Informática y Comunicaciones
- [ ] Comunicación y seguridad
- [ ] Centro de seguridad

Tener diferentes contraseñas para cada servicio es la opción más segura:

- [ ] Verdadero
- [ ] Falso

Soluciones a 'Repasando lo aprendido'

El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger infraestructura computacional (activos de la organización) y todo lo relacionado con esta y a los propios usuarios de la misma, se conoce como:

- [ ] Identidad digital
- [ ] Ciberseguridad
- [ ] Phishing

¿Existen administradores de contraseñas que guardan una copia segura de estas en un ordenador o en la nube?

- [x] Verdadero
- [ ] Falso

¿Cuáles son algunas de las principales amenazas de la identidad digital?

- [ ] La suplementación de identidad
- [ ] La publicación por terceros de informaciones falsas
- [ ] La utilización no consentidad de derechos de propiedad
- [x] Todas son correctas

¿Qué es el LOPD?

- [X] Ley Orgánica 3/2018 de 5 de diciembre Protección de Datos de Carácter Personales y garantía de los derechos digitales
- [ ] Reglamento General de Protección de Datos
- [ ] Ley Orgánica de Derechos personales

Según los consejos de ciberseguridad, cada vez que termines de navegar en una página con tus credenciales, debes cerrar la sesión

- [x] Verdadero
- [ ] Falso

¿Qué es el phishing?

- [ ] El uso indebido de la imagen corporativa, marca u otros elementos por parte de terceros sin permiso del propietario
- [x] La técnica usada para obtener información personal y bancaria de los usuarios suplantando a una entidad legítima como puede ser un banco, una red social o una entidad pública
- [ ] El uso de publicaciones por terceros de informaciones falsas que puede arruinar la reputación online de una persona o marca

Las redes wifi públicas (aeropuertos, cafeterías, bibliotecas, etc.) son seguras ya que cifran la información que se transmite a través de ellas y porque podemos ver quién está conectado a la red.

- [ ] Verdadero
- [x] Falso

Un malware es la forma genérica de llamar a cualquier programa que se ejecuta sin autorización y con objetivos maliciosos (virus, troyanos, gusanos…).

- [x] Verdadero
- [ ] Falso

¿Cuáles son las recomendaciones correctas para no perder nuestra información personal (fotos, vídeos, documentos, etc) de nuestros dispositivos?

- [ ] Has solamente una copia de seguridad en tu espacio de la nube
- [x] Selecciona los archivos deseados, elige el soporte de almacenamiento donde los copiarás, haz la copia de seguridad y repite este proceso periódicamente.
- [ ] Selecciona los archivos que desees almacenar, crea una carpeta en el escritorio de tu ordenador y cópialos ahí.

Qué servicio responsable de la Universidad Pablo de Olavide vela por la seguridad informática de toda la comunidad universitaria

- [x] Centro de Informática y Comunicaciones
- [ ] Comunicación y seguridad
- [ ] Centro de seguridad

Tener diferentes contraseñas para cada servicio es la opción más segura:

- [x] Verdadero
- [ ] Falso

Soluciones a ‘Actividades de práctica’

Eduroam	Este servicio permite que estudiantes, investigadores y personal de las instituciones participantes tengan conectividad Internet a través de su propio campus y cuando visitan otras instituciones participantes
Centro de informática y comunicaciones UPO	Equipo de profesionales de la Universidad Pablo de Olavide que te ayudarán y velarán por tu seguridad digital en el entorno académico
Troyano	Soy un malware eficaz y muy usado. Mi gran arma es que no soy lo que parezco ser.
Seguridad informática	Es el conjunto de herramientas, políticas, conceptos, salvaguardas, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger la infraestructura computacional y todo lo relacionado con esta, así como a los propios usuarios de la misma
Phising	Los ciberdelincuentes captan nuestra atención con alguna excusa con el fin de redirigirnos a páginas web fraudulentas que simulan ser legales con el fin de robar nuestra información personal.